Trust-Based Collaborative Control for Teams in Communication Networks

P. Ballal and F. Lewis, *Fellow, IEEE*
Automation & Robotics Research Institute, University of Texas at Arlington,
7300 Jack Newell Blvd. S., Fort Worth, TX 76118-7115, USA.

ABSTRACT

U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-66 identifies Force Operating Capabilities required for the Army to fulfill its mission for a networked Warfighter concept. Two such capabilities are Battle Command and Battle-space Awareness for which there are expectations (trust) that networked nodes will perform in a certain manner given certain contexts. As an example, for battlefield or disaster area teams in a distributed network, trust is interpreted as a set of relations among the nodes participating in the network activities. Trust establishment in distributed communication networks such as mobile ad hoc networks (MANETs), sensor networks and ubiquitous computing systems is considered to be more difficult than in traditional hierarchical structures such as the Internet and Wireless LANs centered on base-stations and access points. In this paper, we concentrate on trust establishment in self-organized, distributed and resource constrained networks. We model our trust establishment strategy as a bilinear local voting protocol and discuss its behavior, i.e. how trusts spreads in the distributed network, and analyze its convergence behavior based on algebraic graph theory. Then, we show how to incorporate trust into local networked control laws which yields two coupled systems, a bilinear trust dynamics coupled to a local control law. Different team behaviors will emerge automatically depending on the trust each node has for its neighbors. In this paper we give examples of the flocking and formation behavior of nodes in a distributed network.

1. INTRODUCTION

Mission command is the US Army's preferred method for executing battle command and is characterized by decentralized execution in which commanders convey purpose without providing detailed direction on how to perform the task or mission (U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-66). Mission command requires an environment of trust and mutual understanding between agents and empowers subordinate initiative by emphasizing the higher commander's intent. For example, battlefield or disaster area teams may be heterogeneous networks consisting of interacting humans, ground sensors, and unmanned airborne or ground vehicles (UAV, UGV). Developed team scenarios include the War-fighter Information Network-Tactical (WIN-T), DARPA Agile Information Control Environment (AICE), C4ISR Architectures for the War-fighter (CAW), Joint Force Air Component Commander (JFACC) Project, etc. Such scenarios should provide intelligent shared services of sensors and mobile nodes to augment the capabilities of the remote-site mission commander and on-site war-fighter in terms of: (1) extended sensing ranges, (2) sensing of modalities such as IR and ultrasound not normally open to humans, and (3) cooperative control of UAV/UGV to extend the war fighter strike range. Also (4) Automated decision assistance (via, e.g., handheld PDAs) should be provided to the war fighter based on algorithms that only depend on local information from nearest neighbor sensor nodes or humans, yet yield network-wide guaranteed performance.

There is a need to provide means for teams to grow and develop trust through the extensive use of simulation, scenario-driven war games, experiments, and training exercises that challenge leaders and reduce the need to learn "on the job" in actual combat operations (U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-66). As the team members may often be geographically distributed there will be a heightened need for shared conceptualization of teamwork built on trust. Also, given the presence of enemy components and the possibility of node compromise, a *trust consensus* must be reached by the team that determines which nodes to trust, which to disregard, and which to avoid. Trust algorithms for unmanned nodes must be autonomous computationally efficient numerical schemes. However, existing schemes for control of dynamical systems on communications graphs (in the style of work by (Beard and Stepanyan, 2003; Fax and Murray, 2004; Jadbabaie et al., 2003; Lee

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Trust-Based Collaborative Control for Teams in Communication Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Automation & Robotics Research Institute, University of Texas at Arlington, 7300 Jack Newell Blvd. S., Fort Worth, TX 76118-7115, USA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002187. Proceedings of the Army Science Conference (26th) Held in Orlando, Florida on 1-4 December 2008, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**8**	

and Spong, 2007; Olfati-Saber and Murray, 2004; Ren and Beard, 2005; Ren et al., 2005; Saligrama et al., 2006.)) do not take into account trust propagation and maintenance (such as work by (Jiang and Baras, 2006; Theodorakopoulos and Baras, 2006)). Yet it is a fact that biological groups such as flocks, swarms, herds (Reynolds, 1987), do have built-in trust mechanisms to identify team members, team leaders, and enemies to be treated as obstacles or avoided. Cooperative mission planning should involve decisions made in the context of the trust opinions of all nodes, and be based on performance criteria set by human war fighter nodes or team leaders. These performance criteria may change with time depending on varying mission objectives in the field.

Recently, many researchers have worked on problems that are essentially different forms of agreement problems with differences in the types of agent dynamics, properties of graphs and the names of the tasks of interest. In (Fax and Murray, 2004), graph Laplacians were used for the task of formation stabilization for groups of agents with linear dynamics. In (Jadbabaie et al., 2003) directed graphs were be used to represent the information exchange between the agents. In (Beard and Stepanyan, 2003), a linear update scheme was introduced for directed graphs. In (Chopra and Spong, 2006) a Lyapunov-based approach was used to consider stability of consensus synchronization for balanced and weakly connected networks. The work by (Olfati-Saber and Murray, 2004) solved the average consensus problem with directed graphs which required the graph to be strongly connected and balanced. In (Ren and Beard, 2005), it was shown that under certain assumptions consensus can be reached asymptotically under dynamically changing interaction topologies if the union of the collection of interaction graphs across some time intervals has a spanning tree frequently enough. The spanning tree requirement is a milder condition than connectedness and is therefore suitable for practical applications. They also allowed the link weighing factors to be time-varying which provides additional flexibility. In contrast to the aforementioned protocols, this work uses a bilinear protocol for trust consensus in directed graphs.

In this paper, we develop a framework for trust propagation and maintenance in team networks of nodes that yields global consensus of trust under rich enough communication structure graphs. Most of the work in literature considers the graph Laplacian to be static or have time-varying weights which are due to unreliable transmission or limited communication or sensing range. In this paper we consider the case where the graph Laplacian is a time-varying function of the trusts based on the graph connectivity. This makes the trust consensus protocol bilinear.

There has been a tremendous amount of interest in flocking and swarming that has primarily originated from the pioneering work of Reynolds, 1987. The trust consensus protocols developed in this paper is incorporated into cooperative control laws that depend on local information from neighboring nodes, yet yield team-wide desired behavior such as flocking and formations.

This paper is organized as follows. In Section 2 we describe the notions involved in trust graphs and formally devise a bilinear trust consensus protocol in continuous-time and discrete-time. Section 3 contains our main results with the convergence performance for the two consensus protocols. Section 4 gives examples of emerging team behavior using these protocols with a case study on flocking and formations. Section 5 offers our concluding remarks.

2. TRUST PROPAGATION IN GRAPHS

2.1 Trust Graphs

Given a network of N agents or nodes $V=\{v_1,\ldots,v_N\}$ who are to engage in cooperative trust evaluation. Define a trust graph $G_T = (V, E)$, where edge $(v_i, v_j) \in E$ if node v_j obtains a direct trust evaluation about node v_i. Note this is backwards from (Jiang and Baras, 2006; Theodorakopoulos and Baras, 2006). Define the direct trust neighborhood of node v_i as $N_i = \{v_j : (v_j, v_i) \in E\}$, i.e. the set of nodes with edges incoming to v_i. The graph is directed since if node j can obtain a direct evaluation of trust about node i, the reverse may not be true. Given the trust graph, define the graph adjacency matrix $A = [a_{ij}]$ where $a_{ij} = 1$ if e_{ji} is an edge, and $a_{ij} = 0$ otherwise. A is a constant matrix defined by the direct trust relations between nodes. In fact, adjacency matrix A captures the information flow in the trust graph. If there is a directed path, e.g. a sequence of nodes $v_0, v_1, \cdots, v_r$ such that $(v_i, v_{i+1}) \in E, i \in \{0,1,\cdots,r-1\}$, then, node v_r should be able to form an indirect trust opinion about node v_0 based on the opinions of the agents along the path. Likewise, if two paths converge at an agent v_r, each of which contains agent v_0, then v_r has a basis to form a more confident opinion about the trustworthiness of agent v_0 than if there were only a single path.

2.2 Trust Consensus Protocols

We encode the trust opinions an agent i has about other agents in the network as a trust vector $\xi_i \in R^N$

associated with each *node*, with elements indexed by all the nodes about which node *i* has an opinion. That is $\xi_i = [\xi_{ii1}\ \xi_{ii2}...]^T$ where ξ_{ij} is the trust node *i* has for node *j*. Throughout this paper, the trust values ξ_{ij} are assumed to be in [0, 1].

Consider the following trust protocol in continuous-time.

$$\dot{\xi}_i = u_i \tag{1}$$

$$u_i = \sum_{j \in N_i} w_{ij}(\xi_j - \xi_i) \tag{2}$$

In (Ren and Beard, 2005), w_{ij} was taken as $a_{ij}\sigma_{ij}$ where σ_{ij} is a time-varying weighting factor chosen from any finite set. In (Jiang and Baras, 2006), w_{ij} was taken as $a_{ij}c_{ij}$, where c_{ij} is the confidence node *i* has in its trust opinion of node *j*. Hence each node has an associated $[\xi, c]$, i.e. trust and confidence each of which have two operations $(\oplus, \otimes)$ which form a semi-group (Theodorakopoulos and Baras, 2006). In (Jiang and Baras, 2006), the weights c_{ij} were kept constant throughout.

In this paper, we propose the following local voting continuous-time trust protocol,

$$u_i = \sum_{j \in N_i} a_{ij}\xi_{ij}(\xi_j - \xi_i) \tag{3}$$

This protocol is bilinear in the trust values. Note that this defines a graph topology that stays constant, yet the edge weights are equal to ξ_{ij}, the trust that node *i* has for its neighbor node *j*. The weighted adjacency matrix is defined by $W = [w_{ij}] = [a_{ij}\xi_{ij}]$. This defines a graph which has a constant topology given by the adjacency matrix *A*, yet whose edge weights vary as node *i* changes its trust opinion about its neighbor nodes, i.e. this is a weighted version of the trust graph defined by the adjacency matrix *A*. If ξ_i's are scalars, (3) can be rewritten as,

$$\begin{aligned} u_i &= \sum_{j \in N_i} a_{ij}\xi_{ij}(\xi_j - \xi_i) \\ &= \sum_{j \in N_i} a_{ij}\xi_{ij}\xi_j - \sum_{j \in N_i} a_{ij}\xi_{ij}\xi_i \\ &= -(D(t) - W(t))\xi_i \end{aligned}$$

$$\dot{\xi}_i = -(D(t) - W(t))\xi_i = -L(t)\xi_i \tag{4}$$

Here, $D(t)$ is the time-varying in-degree matrix defined as $D(t) = diag\{n_i\}$ where $n_i = \sum_{j \in N_i} a_{ij}\xi_{ij}$, and $W(t)$ is a time-varying weighted adjacency matrix. These matrices are functions of node trusts ξ. $L(t)$ is a time-varying Laplacian matrix defined as $D(t)$-$W(t)$ which is also a function of the node trusts. Note that the node trust vectors $\xi_i(t)$ have nonzero entries ξ_{ij} corresponding to the weights of incoming edges e_{ji}, which have $a_{ij} = 1$, but there may also be nonzero entries $\xi_{ij}(t)$ that do not correspond to edges in the graph. Thus, though a node *i* forms a trust opinion about more and more nodes as trust propagates through the graph, its direct trust neighbors (the graph edges coming into node *i*) never change, and are defined by the adjacency matrix *A*.

Since $\xi_i \in R^N$, we must use Kronecker product (Godsil and Royle, 2001) to write,

$$\dot{\xi} = -(L(t) \otimes I_N)\xi \tag{5}$$

where I_N is an identity matrix of $N \times N$. Here, $\xi = [\xi_1^T \cdots \xi_N^T]^T \in R^{N^2}$ is the overall network trust vector.

The Laplacian $L(t)$ corresponds to a time-varying graph $G(t)$. The initial Laplacian $L(0)$ corresponds to the initial graph $G(0)$. Note that the row sum of $L(t)$ is zero for $\forall t$. Hence, $L(t)$ has a zero eigenvalue corresponding to the right eigenvector of **1**, where **1** is a column vector with all entries equal to one.

We also propose the following nonlinear local voting discrete-time trust consensus protocol based on the Vicsek model (Vicsek et al., 1995),

$$\xi_i(k+1) = \xi_i(k) + \frac{1}{n_i + 1}\sum_{j \in N_i} a_{ij}\xi_{ij}(\xi_j - \xi_i) \tag{6}$$

which can be rewritten in the scalar case as,

$$\begin{aligned} \xi_i(k+1) &= (I - (I + D(k))^{-1}L(k))\xi_i(k) \\ \xi_i(k+1) &= F(k)\xi_i(k) \end{aligned} \tag{7}$$

where

$$F(k) = I - (I + D(k))^{-1}L(k) = (I + D(k))^{-1}(I + W(k))$$

Since $\xi_i \in R^N$, we must use Kronecker product to write,

$$\xi(k+1) = (F(k) \otimes I_N)\xi(k) \tag{8}$$

Here, $\xi = [\xi_1^T \cdots \xi_N^T]^T \in R^{N^2}$. Note that $F(k)$ is a time-varying stochastic matrix that depends on the trust values ξ_{ij}. The matrix $F(k)$ corresponds to a time-varying graph $G(k)$ with Laplacian $L(k)$ $F(0)$ corresponds to the initial graph $G(0)$ with initial Laplacian $L(0)$. For each k, $F(k)$ has a eigenvalue of one corresponding to the right eigenvector of **1**, where **1** is a column vector with all entries equal to one. Even if $F(k)$, $F(k\text{-}1)$, $F(k\text{-}2)$,…, $F(0)$

are time-varying, the graph topology remains the same, only the weights in F change, which we prove in Section 3.

3. CONVERGENCE OF TRUST

We say that a protocol achieves (asymptotic) consensus if for every i, j one has $\xi_i(t) \to \xi_j(t) \to \xi_*$ in continuous-time, $\xi_i(k) \to \xi_j(k) \to \xi_*$ in discrete-time, where ξ_* is called the consensus trust vector value. If this occurs, then in the limit one has $\xi_{ip} = \xi_{jp}$ for all i, j so that all nodes arrive at the same trust value for each other at node p. To prove the trust consensus, we need to have the following assumption.

Assumption 1: In the trust graph G_T, $\xi_{ij}(0) > 0$ if $a_{ij} = 1$.

The main result of this paper is that the bilinear trust protocol (5) for continuous-time and (8) for discrete-time achieve asymptotic consensus for a trust graph G_T if and only if the initial graph $G(0)$ has a spanning tree. Under Assumption 1, this is equivalent to the trust graph G_T containing a spanning tree. We are of course inspired by (Ren and Beard, 2005), which covers the case of linear integrator dynamics.

Two nonnegative matrices are said to be of the same type if their zero elements are in the same locations (Ren and Beard, 2005). We will use the notation $P \sim Q$ to denote that P and Q are of the same type. Two graphs on the same nodes are of the same type if their edge sets are the same.

3.1 Consensus of the Discrete-Time Protocol

In this section, we prove that the trust protocol in (8) achieves asymptotic consensus if and only if the initial graph $G(0)$ has a spanning tree. Assumption 1 means that G_T and $G(0)$ are of the same type, i.e. $G_T \sim G(0)$. For each $F(k)$ associate a set of graphs $\{G(k)\}$. Now, F is a time-varying function of the trusts with the initial trust vectors for each node $\xi_i(0)$ in [0, 1]. Consider the local voting discrete-time trust consensus scheme based on the Vicsek model given in (8). Let $F(0)$ represent the initial directed graph $G(0)$. If $\xi_{ij}(0)$ is an edge in $G(0)$ then $\xi_{ij}(k)$ is an edge for all $G(k)$, for $k \geq 0$. This is formalized in the next result.

Lemma 1: Consider a network with initial graph $G(0)$ running the discrete-time consensus scheme in (8) with initial condition $\xi(0)$. Let $\xi_{ij}(k) > 0$ for some time instant $k \geq 0$. Then $\xi_{ij}(k+1) > 0$. As a result, $G(k)$ for $k \geq 0$ are all of the same type.

Proof: From (8), each updated node trust is a weighted average of its neighboring trust values such that the weights are nonnegative and less than 1, because the row sum of $F(k)$ and $F(k) \otimes I_N$ is 1, i.e. they are stochastic (Wolfowitz, 1963). Protocol in (8) can be rewritten for each state as,

$$\xi_{ij}(k+1) = \sum_l f_{il}(k)\xi_{lj}(k)$$
$$= f_{ii}(k)\xi_{ij}(k) + \sum_{l \neq i} f_{il}(k)\xi_{lj}(k)$$

where $f_{ij}(k)$ is the $(i,j)^{th}$ element of $F(k)$. Then by definition of $F(k)$, we know that, $0 \leq f_{ij}(k) < 1$, for $i \neq j$ and $0 < f_{ii}(k) \leq 1$. Also, $f_{ii} = \frac{1}{1+n_i} > 0$. Hence, if $\xi_{ij}(k) > 0$, the first term is always positive. The second term is a weighted average which once again is always nonnegative for non-zero initial trusts. Therefore, for $k \geq 0$, if $\xi_{ij}(k) > 0$, $\xi_{ij}(k+1) > 0$.

Thus, if $\xi_{ij}(0) > 0$ is an edge weight for $G(0)$, then $\xi_{ij}(k) > 0, \forall k > 0$ is an edge weight for $G(k)$. Therefore, $G(k)$, $\forall k \geq 0$ are all of the same type. ■

Theorem 1: Let $\xi_{ij}(0) > 0$ if $a_{ij} = 1$. Then the discrete-time trust protocol in (8) achieves a trust consensus for $\xi_{ij}(k)$ if and only if the trust graph G_T has a spanning tree.

Proof: Now $G(0)$ has a spanning tree if and only if $G(k)$, $\forall k > 0$, has a spanning tree by Lemma 1. Under Assumption 1, this is equivalent to the trust graph G_T containing a spanning tree. This is a necessary and sufficient condition for the union of graphs over any finite time interval to have a joint spanning tree. Therefore, Theorem 3.8 in (Ren and Beard, 2005) proves the result. ■

Example 1: Consider a six node network as shown in Figure 1. Let the initial trust vectors $\xi_i(0) \in R^6$ have elements selected randomly in [0, 1].

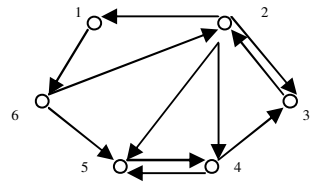

Figure 1. A Six Node Directed Graph

Figure 2 shows convergence of trust in a six node network with 6 states using the discrete-time protocol given by (8). ■

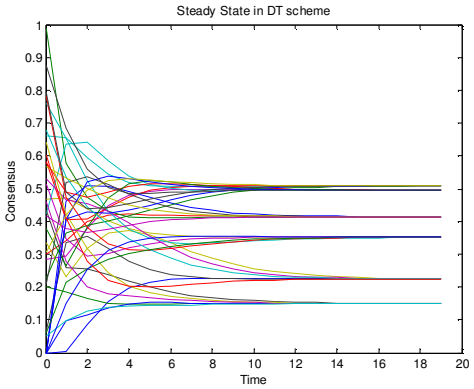

Figure 2. Trust Consensus in the Discrete-time Scheme

3.2 Consensus of the Continuous-Time Trust Protocol

In this section, we prove that the bilinear trust protocol in (5) achieves asymptotic consensus for a trust graph G_T if and only if the initial graph $G(0)$ has a spanning tree. Assumption 1 means that G_T and $G(0)$ are of the same type, i.e. $G_T \sim G(0)$. For each $L(t)$ associate graph $G(t)$. For the continuous-time scheme, one has $L(t)=[l_{ij}(t)]$, the diagonal elements of $L(t)$ are positive, the off-diagonal elements are negative and $\sum_j l_{ij} = 0$. Let $\phi(t,t_0)$ be the corresponding transition matrix of $L(t)$ defined as

$$\phi(t,t_0) = I + \int_{t_0}^{t} L(\sigma 1)d\sigma 1 + \int_{t_0}^{\sigma 1} L(\sigma 2)d\sigma 2 d\sigma 1 + \ldots.$$

From (Ren and Beard, 2005), we know that the transition matrix $\phi_L(t,t_0)$ of $L(t)$ is a nonnegative stochastic matrix with positive diagonal elements. Also, the corresponding transition matrix of $L(t) \otimes I_N$ is $\phi_L(t,t_0) \otimes I_N$ which is once again a nonnegative stochastic matrix with positive diagonal entries. Along the same lines as in Lemma 1, we can prove the following Lemma.

Lemma 2: Consider a network with initial graph $G(0)$ running the continuous-time protocol (5) with initial node trust vectors $\xi_i(0)$. Let $\xi_{ij}(0) > 0$. Then for $\forall t > 0$, $\xi_{ij}(t) > 0$. As a result, $G(t)$ for $t \geq 0$ are all of the same type.

Proof: Solution of (5) can be written as $\xi(t) = (\phi_L(t,0) \otimes I_N)\xi(0)$. This can be rewritten for each state as,

$$\xi_{ij}(t) = \phi_{Lii}(t,0)\xi_{ij}(0) + \sum_{l \neq i} \phi_{Lil}(t,0)\xi_{lj}(0) \qquad (9)$$

Here, the diagonal elements of $\phi_L(t,0) \otimes I_N$ are always positive and therefore the first term in the RHS of Equation (9) will always be positive for $\xi_{ij}(0) > 0$. The second term in the RHS of Equation (9) is always nonnegative since $\phi_L(t,0) \otimes I_N$ is a nonnegative stochastic matrix with positive diagonal entries (Wolfowitz, 1963). Thus, if $\xi_{ij}(0) > 0$ is an edge weight for $G(0)$, then $\xi_{ij}(t) > 0, \forall t > 0$ is an edge weight for $G(t)$. Therefore, $G(t)$, $\forall t \geq 0$ are all of the same type. ■

Theorem 2: : Let $\xi_{ij}(0) > 0$ if $a_{ij} = 1$. Then the continuous-time trust consensus protocol in (5) achieves trust consensus for $\xi_{ij}(t)$ if and only if the trust graph G_T has a spanning tree.

Proof: Now $G(0)$ has a spanning tree if and only if $G(t)$, $\forall t$ has a spanning tree by Lemma 2. Under Assumption 1, this is equivalent to the trust graph G_T containing a spanning tree. Also $\varphi_L(t,0)$ is a continuous function of $L(t)$ for the interval $[0, t]$. This is a necessary and sufficient condition for the union of graphs over any finite time interval to have a joint spanning tree. Therefore, the result (Theorem 3.2) in (Ren et al., 2005) proves the result. ■

Example 2: Consider the same six node network as shown in Figure 1. Let the initial $\xi(0) \in R^6$ be the same as in Example 1. Figure 3 shows convergence of trust in a six node network with six states using the continuous-time protocol given by (5). It can be observed that the discrete-time and the continuous-time schemes give different consensus values for the same initial conditions. ■

3.3 Relation of the Continuous and Discrete-time Protocols

The Laplacian L in the continuous-time protocol is related to the stochastic matrix F in the discrete-time protocol at each time instance. As shown in Figures 3 and 4, the trust consensus using (8) and (5) do not converge to the same consensus. This is because the graph represented by $F(k)$ is not the same as the graph represented by $L(t)$. In fact,

$$F = I-(I+D)^{-1}L \qquad (10)$$

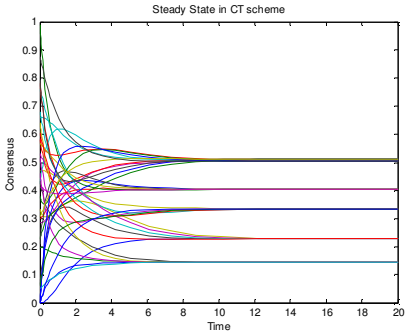

Figure 3. Trust Consensus in the Continuous-time Scheme

It can be seen that the discrete-time consensus protocol is the first order Euler approximation of the continuous-time protocol given by,

$$\dot{\xi}_i = -(I+D)^{-1} L \xi_i \qquad (11)$$

If this protocol is used, both the continuous-time protocol in (11) and the discrete-time protocol in (7) would approximately converge to the same consensus. See Figures 4 and 5. Here for the same network in Figure 1, initial trusts $\xi(0) \in R^6$ are selected randomly in [0, 1].

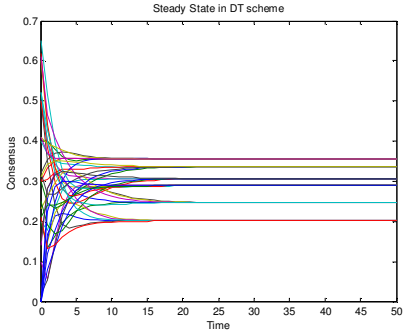

Figure 4. Trust Consensus in the Discrete-time Scheme

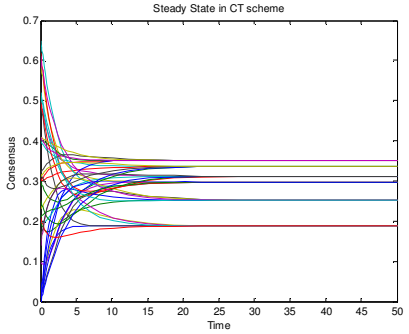

Figure 5. Trust Consensus in the Continuous-time Scheme using scheme (11)

4. TEAM BEHAVIORS BASED ON TRUST

Different team behaviors will emerge automatically depending on the trust each node has for its neighbors, e.g. flock (Tanner et al., 2003a, 2003b), or swarm (Gazi and Passino, 2003, 2004) with trusted neighbors, follow trusted leader, avoid enemy node. In this section we explore flocking behavior and formations in a distributed network of agents.

4.1 Flocking

The flocking model consists of three steering behaviors which describe how an individual agent maneuvers based on the positions and velocities of the neighboring flock-mates (Reynolds' rules (Reynolds, 1987)):

1. **Separation:** steer to avoid closely located flock-mates.
2. **Alignment:** steer towards the average heading of local flock-mates.
3. **Cohesion:** steer to move toward the average position of local flock-mates.

The superposition of these three rules results in all agents moving in a formation (Chopra and Spong, 2006, Dunbar and Murray, 2006), with a common heading while avoiding collisions. Generalizations of this model include a leader follower strategy, in which one agent acts as the group leader and the other agents would just follow the aforementioned rules, resulting in leader following.

Define a control graph G_C and consider the node dynamics having local rule,

$$\dot{x}_i = \sum_{j \in N_i^c} k_{ij} \xi_{ij} (x_j - x_i) \qquad (12)$$

with k_{ij} some control graph edge weights (control gains) and N_i^c the control neighborhood of node i. Suppose the trust of node i for node j satisfies the bilinear trust local voting dynamics,

$$\dot{\xi}_i = \sum_{j \in N_i^t} a_{ij} \xi_{ij} (\xi_j - \xi_i) \qquad (13)$$

with N_i^t the trust neighborhood of node i. The structure of the trust graph G_T is defined by the adjacency matrix $A=[a_{ij}]$. Note that (12) and (13) is a coupled system.

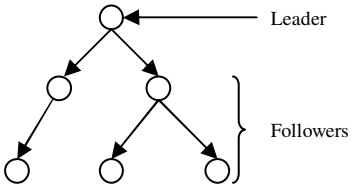

Figure 6. Tree network with one leader and five followers

Example 3: Let x_i represent the heading of node i in a formation. Consider the formation graph shown in Figure 6. First we run the trust update protocol above on the case of fully trusted nodes. That is, the initial trust vectors $\xi_i(0)$ of the nodes have all entries positive or zero. Then, as the trusts change, the edge weights change but stay positive, so the graph structure is preserved. Then, all nodes converge to the initial heading value $x_1(0)$ of the leader.

Let the initial $\xi(0) \in R^6$ selected randomly in [0, 1]. Figure 7(a) shows that the trusts of the followers converge to the initial trusts of the leader node. Let the heading of each node be $x \in R^1$. Figure 7(b) shows the heading consensus in this network. As mentioned before, the heading of the followers converge to the heading of the leader.

Figure 8 shows the motion of each node with the follower node headings converging to the heading of the leader node. Here the velocity of each node is considered to be the same. ■

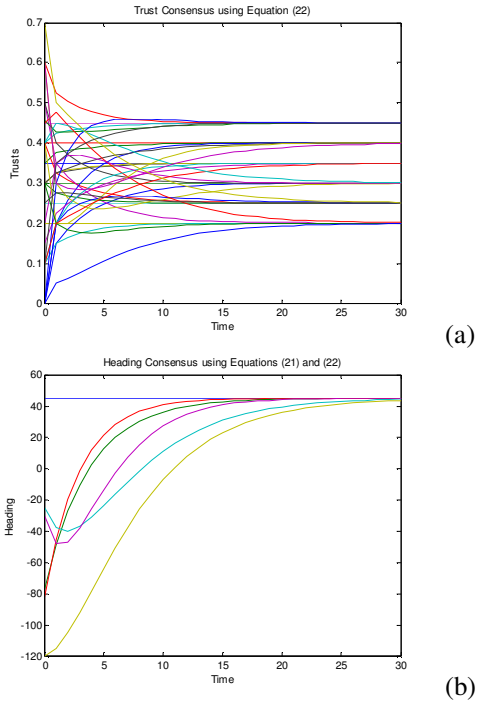

Figure 7. (a)Convergence of trusts of all the nodes, (b) Convergence of headings of all the nodes in a tree network

4.2 Formations

A formation of autonomous vehicles refers to a set of spatially distributed vehicles whose dynamic states are coupled through a common control law.

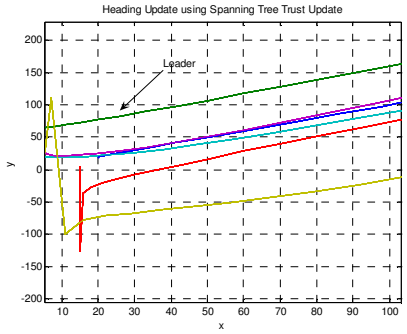

Figure 8. Convergence of headings of all the nodes in a tree network

Following shows an easier way to maintain formations in a desired configuration. Moreover, as the desired configuration changes, the formation can quickly be moved into the new desired structure.

Let the states x in (12) be defined as, $x = [(x_1^d)^T (x_2^d)^T ... (x_N^d)^T]$ with $x_i^d \in R^3$, the desired (x,y,z) position of node i in the formation with respect to the leader. All other nodes take their initial states as their own actual initial positions.

Example 4: For the same tree network in Example 3, we want the desired positions of the nodes in the hexagonal formation structure. Let the initial state of the leader $x_1(0)$ contain the desired formation positions of all the other nodes in the network in 2D, i.e. (x, y). If we run the coupled node dynamics and bilinear trust update in (12) and (13) (and using Kronecker product), all nodes converge to the initial state of the leader, i.e. to their desired formation positions as shown in Figure 9.

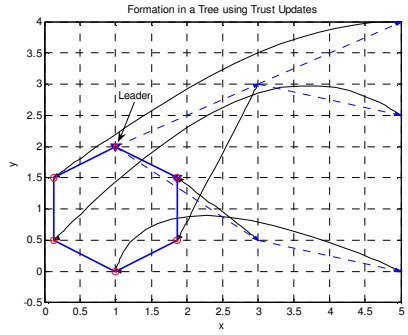

Figure 9. Convergence of positions of all the nodes in a tree network to a hexagon formation

If the desired relative positions of all or some of the nodes change, then the leader simply resets $x_{ss} = x_1(0)$, and all nodes will automatically converge to the new consensus trust and positions, as specified by the leader in its initial state vector. ■

5. CONCLUSIONS

This paper considered the problem of trust establishment and consensus in a distributed network. Directed graphs were used to represent the information exchange between the nodes. We proposed a continuous-time and a discrete-time bilinear trust update scheme for trust consensus. We described the convergence characteristics of these schemes in terms of the steady state and the convergence bound. We provided an application of these update schemes in team behaviors such as flocking and formations. As a part of future study, we would like to find the exact steady-state of trust in these protocols in terms of the Eigenvectors of F and L. Also, in this paper we considered the trusts to be in [0, 1]. As a part of the future work, we would like to have trusts in [-1, 1] where 1 represents complete trust, 0 represents no opinion and -1 represents complete distrust. One way of solving this would be to use a one-step distrust model where all the nodes connected to a distrusted node are disregarded or to use graph pruning and reconnection to remove the distrusted node from the original network.

ACKNOWLEDGEMENTS

This work was supported by ARO grant ARO W91NF-05-1-0314 and the Army National Automotive Center, and NSF grant ECCS-0801330

REFERENCES

Beard, R. and Stepanyan, V., 2003: Synchronization of information in distributed multiple vehicle coordinated control, *Proc. IEEE Conf. Decision and Control.*, pp. 2029-2034.

Chopra, N. and Spong, M.W., 2006: Passivity-based control of multi-agent systems, *Advances in Robot Control: From Everyday Physics to Human-Like Movements.*, ed. S. Kawamura and M. Svinin, Springer-Verlag, Berlin, pp. 107-134.

Dunbar, W.B. and Murray R.M., 2006: Distributed receding horizon control for multi-vehicle formation stabilization, *Automatica.*, vol. 42, pp. 549-558.

Fax, J.A. and Murray, R.M., 2004: Information flow and cooperative control of vehicle formations, *IEEE Trans. Automatic Control*., vol. 49, no. 9, pp. 1465-1476.

Gazi, V. and Passino, K.M., 2003: Stability analysis of swarms, *IEEE Trans. Automatic Control*., vol. 48, no. 4, pp. 692-697.

Gazi, V. and Passino, K.M., 2004: A class of attractions/repulsion functions for stable swarm aggregations, *Int. J. Control*., vol. 77, no. 18, pp. 1567-1579.

Godsil, C. and Royle G., 2001: Algebraic Graph Theory, *Springer Graduate Texts in Mathematics.*, no. 207, New York.

Jadbabaie, A., Lin, J. and Morse, A.S., 2003: Coordination of groups of mobile autonomous agents using nearest neighbor rules, *IEEE Trans. Automatic Control*., vol. 48, no. 6, pp. 988-1001.

Jiang, T. and Baras, J.S., 2006: Trust evaluation in anarchy: a case study on autonomous networks, *Proc. Infocom, Barcelona*., 2006.

Lee, D. and Spong, M.W., 2007: Stable flocking of multiple inertial agents on balanced graphs, *IEEE Trans. Automatic Control*., vol. 52, no. 8, pp. 1469-1475.

Olfati-Saber. R, and Murray, R.M., 2004: Consensus problems in networks of agents with switching topology and time-delays, *IEEE Trans. Automatic Control*., vol. 49, no. 9, pp. 1520-1533.

Ren, W. and Beard, R.W., 2005: Consensus seeking in multiagent systems under dynamically changing interaction topologies, *IEEE Trans. Automatic Control*., vol. 50, no. 5, pp. 655-661.

Ren, W., Beard, R.W. and Kingston, D., 2005: Multi-agent Kalman Consensus with Relative Uncertainty, *Proceedings of ACC*.

Reynolds C., 1987: Flocks, herds and schools: a distributed behavioral model, *Computer Graphics*., 2 1 (4):25-34.

Saligrama, V., Alanyali, M., and Savas, O., 2006: Distributed detection in sensor networks with packet losses and finite capacity links, *IEEE Trans. Signal Proc.,* vol. 54, no. 11, pp. 4118-4132.

Tanner, H., Jadbabaie, A. and Pappas G., 2003a: Stable flocking of mobile agents, Part i: Fixed Topology, *Proc. IEEE Conf. Decision and Control*, Maui, HI, pp. 2010-2015.

Tanner, H., Jadbabaie, A. and Pappas, G., 2003b: Stable flocking of mobile agents, Part ii: Dynamic Topology, *Proc. IEEE Conf. Decision and Control*, Maui, HI, pp. 2016-2021.

Theodorakopoulos, G. and Baras, J.S., 2006: On trust models and trust evaluation metrics for ad hoc networks, *IEEE J. Selected Areas in Communications.,* vol. 24, no. 2, pp. 318-328.

US Army Training and Doctrine Command (TRADOC)., March 2008: Pamphlet 525-66., "Future Operational Capabilities," Fort Monroe, VA.

Vicsek, T, Czirok, A., Jacob, E., Cohen I. and Schochet O., 1995: Novel type of phase transitions in a system of self—driven particles," *Phys. Rev. Lett*., vol 75, pp.1226-1229.

Wolfowitz J., 1963: Products of indecomposable, aperiodic, stochastic matrices, *Proc. Amer. Math. Soc*., vol. 15, pp. 733-736.